Symantec

Do State and Local Governments Have A Security Problem?

Uncover threats and protect your organization.

Government agencies are streamlining existing business processes and modernizing legacy applications at a record pace, motivated by:

- Compliance with regulatory and industry mandates
- Delivery of transparent and more efficient government services to state citizens
- Cost reduction initiatives using cloud services, mobile and self-service portals
- Coordinating efforts and information sharing across multiple levels of government

A CYBER BREACH EPIDEMIC?

Cyber security concerns remain as Government agencies are:

Experiencing challenges recruiting and retaining qualified security professionals	Concerned about securing emerging technologies such as cloud and mobile	Dealing with aging IT professionals set to retire in the coming years

And on the constituent side:

44% of US citizens are dissatisfied with the quality of online public services

WHY TARGET GOVERNMENTS?

Attackers Are After:

Financial Information

Confidential Information

Health/Medical Records

Disruption/Denial of Services

Critical infrastructure services:

- Large scale municipal services such as power, water, sewer and public safety systems are increasingly connected
- Vulnerabilities in these systems can lead to disruption of public services, potential loss of life and diminished trust in government

Identity and health information is valuable:

One medical record can fetch $50 in the underground economy, which is 10x the value of a live credit card number

Governments are vulnerable to insider threat:

The confidential nature of much government information increases the risk of malicious or accidental insider threat

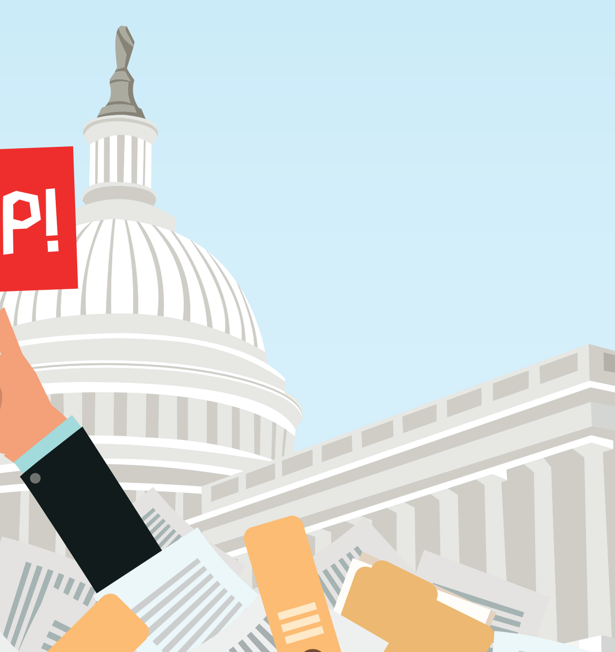
THE CRIMINAL ELEMENT

Malware and attack kits are now available to criminals as a service – little expertise required

The underground black market is thriving, and prices remain stable, indicating a solid supply of stolen information

Dramatic increase in the number of ransomware and cryptoware attacks

PAYING A HEAVY COST



- Globally, organizations run a 28 percent chance that they'll be hit with a data breach, suffering an average cost of $3.86 million, up 6.4 percent from the year before.
- For public sector organizations specifically, the total average cost of a data breach was **$2.3 million**, with an average cost of **$75 per record**.
- Overall, the mean time to identify a breach was **190 days**, and the mean time to contain a breach was **57 days**, according to the survey.

The impact of a government agency breach is more than just a dollar figure

ISTR
Internet Security Threat Report

Volume
23

New and Emerging Threats

Ransomware and Cryptojacking
Supply Chain
Mobile
Cloud
IoT
Critical Infrastructure
Elections Security

READ THE ISTR

Solving the Security Problem

Symantec can help prevent data breaches before they happen by:

Securing access to data through two-factor authentication

Protecting data in the cloud and on mobile devices

Assuring confidentiality of government-held information

Providing threat intelligence and monitoring to get ahead of emerging threats

For more information about Symantec

LEARN MORE ↘

Symantec™

Sources:
Ponemon report: https://statescoop.com/state-it-leaders-review-ponemons-2018-cost-of-a-data-breach-study/
Symantec Internet Security Threat Report, vols. 19+20
Medscape Medical News, "Stolen EHR Charts Sell for $50 Each on Black Market", April 2014
Ponemon Institute, "Cost of Data Breach Study, 2015"
New York Times article "The Cost to Consumers of a Data Breach", 4/30/2013
Accenture White Paper "Digital Government – Pathways to Delivering Public Services for the Future